LIGO Identity Management: Some Status and Trends

Scott Koranda for LIGO

LIGO and University of Wisconsin-Milwaukee

March 8, 2010
LIGO-XXXXXXXX

Why the LIGO Identity Management Project?

- *Unburden users from requesting, retrieving, and managing X.509 certificates and keys*
- Enable finer-grained authorization
- More control over revocation of access and credentials

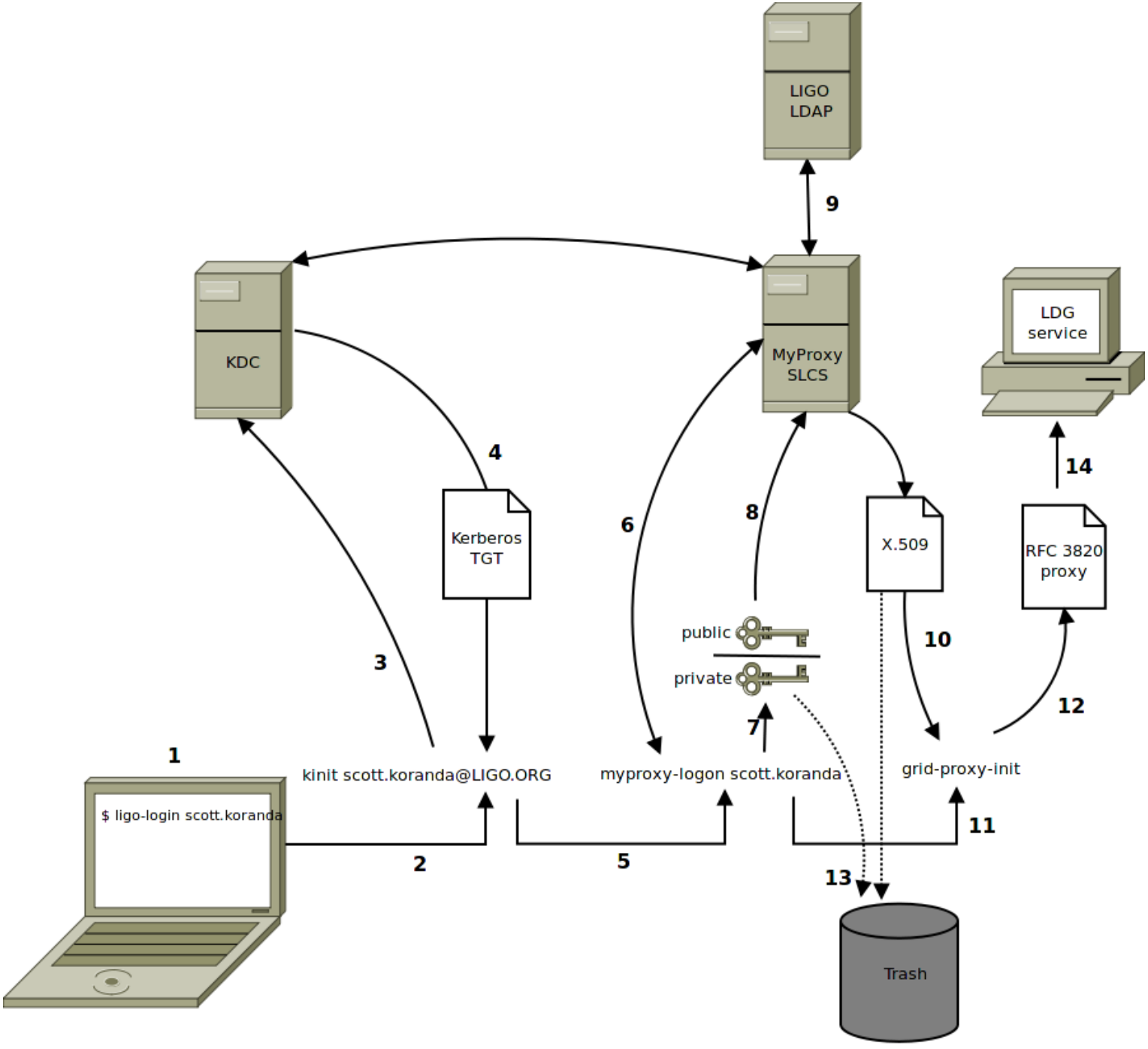
Trend: Grid is only a tool, not THE tool

- Wikis and collaboration tools *as important as grid* for extracting science from data
- Eg. some workflows generate custom Javascript portals for examining results
- Eg. some workflows generate wiki contents to POST
- Grid, web, and CL spaces must seamlessly work together for users
- Driving LIGO Identity Management Project
  - single credential across grid, web, and command line
  - as much single sign-on as possible

LIGO Identity Management Project

Knit together existing technologies and tools

- @LIGO.ORG Kerberos realm
  - single identity (scott.koranda@LIGO.ORG)
  - SSO in command line space
- Grouper from Internet2
  - group-based authorization
  - reflected into distributed LDAP network
- Shibboleth from Internet2
  - login via Kerberos and mod_auth_kerb
  - SSO across web space
  - attributes (groups) pulled from LDAP for fine-grained authz
- MyProxy and GridShib
  - MyProxy in CA and short-lived credential service (SLCS) mode
  - SSO across grid space
  - attributes (groups) pulled from LDAP for fine-grained authz
- Sympa for email management


LIGO
LDAP
9
KDC
MyProxy
SLCS
LDG
service
4
Kerberos
TGT
6
8
X.509
RFC 3820
proxy
14
public
private
10
3
12
7
1
kinit scott.koranda@LIGO.ORG
myproxy-logon scott.koranda
grid-proxy-init
$ ligo-login scott.koranda
11
2
5
13
Trash

Status March 2010:

- Kerberos KDCs in production at 5 sites
- LDAP servers in production at 5 sites
- Transition to Sympa email in progress
- Main git repository accepts both proxy and kerb
- One Shibboleth IdP in production
- Three major LIGO wikis integrated into Shib SP
- Number of smaller web resources served via Shib SP
- LIGO root CA, service CA, and one SLCS CA configured
- No SLCS in production...hopefully summer

Trend: New framework for building grid services

- Apache httpd + mod_ssl + mod_wsgi + Python code
- `export OPENSSL_ALLOW_PROXY_CERTS=1` for httpd
- mod_ssl only for authentication, rolled our own authz
- Used for new metadata and data finding services
- Extremely pleased with this approach

Trend: Services live in ALL spaces

Single identity is just the begining, but an important enabler...

Going forward is the LIGO service model this?

- Apache httpd + mod_ssl + REST $\leftarrow$ grid, CL
- Apache httpd + mod_shib + REST $\leftarrow$ web
- Javascript in browser (ala AJAX) $\leftarrow$ UI
- XMPP $\leftarrow$ mobile devices?

Supplemental Slides

Hi Scott, Warren,
Thank you for your detailed replies and very sorry for not being able to get back in a timely fashion. I ran the command openssl x509 -in $HOME/.globus/usercert.pem -noout -text but it returned an error message saying 'Error opening certificate ... unable to load certificate.' (message below:)

Hi Warren,
The e-mail is attached below. When I click on the "import your certificate", it returns a "Add Certificates" pop-up that asks whether we want to add certificates to a key chain. The keychain options are: login, Microsoft_Intermediate_Certificates, System and X509Anchors. It also opens a panel as attached below. I am not certain how the import is happening in this system. I do not see any .p12 file in my directories and hence the subsequent export commands do not work. Sorry for bothering you. If you have any directions, please let me know. Thanks very much in advance,

Hi Warren, All, I tried out all suggestions, but nothing seemed to work. I don't know what went wrong, but I think perhaps it will be better that my current certificate is cancelled and I apply for a new one? Please let me know if this sounds the right way to proceed. In case we do this, should I request a renewal by typing cert-renew or (because the previous one didn't work) I should type a new request command? Thanks in advance for your advice. Sincerely,

Sorry, Kent. I will submit the new application soon.
Regards,